A Practical Guide to Deploying SecOps Automation

paloalto NETWORKS | CORTEX XSOAR®

Table of Contents

Welcome to the dynamic realm of security automation. In today's rapidly evolving cybersecurity landscape, manual processes alone are insufficient in safeguarding against the ever-increasing spectrum of threats. The necessity for efficiency, accuracy, and scalability has driven security practitioners to embrace automation as a pivotal ally.

However, despite understanding the value of automation, many SecOps teams encounter a roadblock: they may lack the necessary experience to confidently embark on their automation journey.

Recognizing this challenge is crucial. While the potential benefits of automation are clear, the skills gap within SecOps teams presents a significant obstacle. Addressing this hindrance is key to unlocking the potential of automation in strengthening cybersecurity defenses—which is where this guide comes in to help you navigate the automation journey successfully. The following tips are pulled from real-world experiences across thousands of deployments.

Now, let's get started.

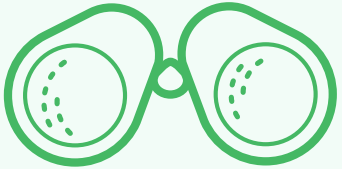
Before You Embark on Your Automation Journey, Here Are Some Things to Consider

These questions will help optimize the move toward automation for you and your organization:

- What are your existing policies and processes?
- What tools do you use daily?
- Who needs to be involved in resolving the incident?
- How can you standardize your processes so they're repeatable and consistent?
- What are your policies and procedures around incident assignment?
- How are you communicating incidents internally?

When analyzing workflows, consider:

- Is an expert needed to interpret or triage the data?



Clearly defining the scope helps in resource allocation, determining the necessary skill sets, and ensuring the team receives adequate training.

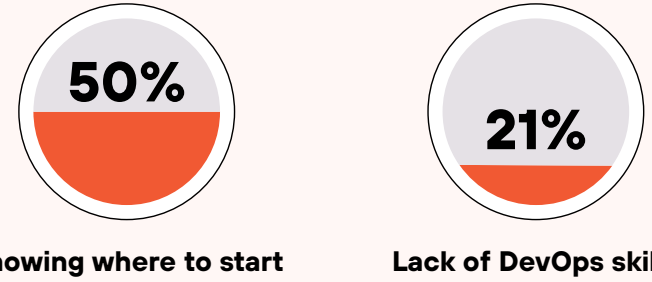
- Are tasks in the workflow repeatable and standardizable?
- Will automating this workflow drastically speed up response?
- Are people needed for testing?

Start Simple

To begin your automation journey, start with tasks that deliver significant value. Consider automating repetitive tasks such as information collection, sandbox reports, queries across various tools, and communication with other teams. Assign an owner for each use case to ensure accountability:

- Are there time-consuming tasks that are part of a larger workflow?
- Are there tasks that impact operations if forgotten?

Tackle these before you try automating a workflow end to end. Can't code? Start with prebuilt playbooks and integrations. Cortex XSOAR has tons to choose from, covering a wide range of common use cases. A visual editor makes it easy to make edits without touching code. These building blocks, such as entity enrichment, indicator blocking, and hunting playbooks, can be reused across multiple use cases, providing immediate value.



"Not sure where to start" is the number one reason for not deploying security automation, with 50% of respondents saying this was their most significant obstacle. Lack of budget and requisite skills were each named as barriers to automation by 21% of respondents. Fourteen percent said management does not understand the need. Twenty-nine percent say they are **"managing fine with current processes."**[1]

Figure 1: What's holding back security automation?

Ease into It

Take a crawl-walk-run approach, gradually automating more steps as you become comfortable with the platform. When implementing cybersecurity automation, particularly with security orchestration, automation, and response (SOAR) solutions, choosing the right automation tool is critical. Start small with a proof of concept (PoC) to demonstrate the benefits. Develop and test automation playbooks, integrating them with existing security tools and systems.

1. *The State of Security Automation*, Palo Alto Networks, December 2, 2021.

Size Doesn't Matter

Automation benefits organizations of all sizes. Mature processes are helpful but not mandatory. Automation can free up time for handling complex tasks even in smaller organizations. Lean on out-of-the-box playbooks and integrations like those in the Cortex Marketplace in the beginning, then tackle more complex projects once you gain confidence and have field-tested a few simple ones. Start with automating simple tasks, moving to end-to-end workflows, and ultimately more complex use cases as you progress.

Be Predictable

Automated workflows, like Cortex XSOAR playbooks, ensure that processes produce the same outputs, the same way, every time. This ensures consistency in response and speeds the onboarding of new security operations center (SOC) analysts, with documented best practices codified into the playbooks. Consistent workflows make it easier to swap out point products, minimizing operational downtime. Regardless of automation, having well-documented and standardized security processes is pivotal, as it improves team efficiency and helps manage incidents effectively.

Peer Review and Approval

The Value of Peer Review

Peer review is a critical step in ensuring the effectiveness of your use cases. By involving colleagues and other teams in your organization, you can identify issues and missed steps, leading to improved automation.

Managerial Approval and Production Deployment

Before deploying your automated workflows into production, they should undergo managerial approval. Consider a development-to-production workflow and track time-sensitive tasks as needed. Determine if service-level agreements (SLAs) should be tracked for follow-ups or remediation actions.

Defining When an Incident Is Closed

Clearly define when an incident is considered closed, and ensure this is integrated into your playbook. If you close incidents on external systems, include this as a final step in your playbook. Consider where an analyst needs to step in to make a decision so you can build that into your workflow.

Get a Champion

Starting small gets you quick wins to justify your investment. However, to take it to the next step, you need stakeholder buy-in to effect real digital transformation in your SOC. XSOAR users who succeed in transforming their SOCs dedicate resources to their teams to drive automation progress and identify areas where automation can be a business enabler.

Invest in Training

Investing in training for cybersecurity automation is a strategic imperative for organizations operating in today's ever-evolving digital landscape. Traditional manual approaches to cybersecurity are no longer sufficient, making it crucial to equip cybersecurity professionals with the skills and knowledge required to harness the full potential of automation.

Automation offers advantages such as swift threat detection and response, heightened accuracy, reduced human error, and a reduced overall workload for staff. This is particularly significant in light of the widening skill gap within the cybersecurity field. With a shortage of qualified professionals, automation can alleviate the resource crunch by enabling existing personnel to manage a broader range of tasks efficiently and, more importantly, prevent employee burnout.

Size Doesn't Matter: Automation for All

The Role of Process Maturity

While mature processes are helpful, they aren't a prerequisite for automation success. Even smaller organizations can benefit from automation. The more you automate, the more you start to refine your processes and the more efficient you become, allowing you to focus on complex tasks that require human expertise.

Automation Benefits Every Organization

Automation streamlines workflows and enhances efficiency, making it valuable for organizations of all sizes. By automating mundane tasks, such as enrichment and password resets, you can free up time to focus on critical security issues.

Mature processes are helpful but also not mandatory. Automation can free up time for handling complex tasks even in smaller organizations. Lean on out-of-the-box playbooks and integrations like those in the Cortex Marketplace in the beginning, then tackle more complex projects once you gain confidence and have field-tested a few simple ones.

What Is Automation?

"It's a very hard thing to answer. I mean, obviously it's taking care of something automatically—but [it doesn't] live in any one place. And that's what makes it hard to answer. So, a lot of people think about, you know, the alert pipeline or the IR [incident response] process as a very linear stage of steps, right? Automation plays a role in that, in multiple places ... And then we're also automating processes in and around the SOC itself so certain procedures are being handled behind the scenes and don't need to be handled by our SOC analysts. That can be governance or audit-related, notifications and alerts of, you know, program or platform health. Automation to us generally is in service of expediting the time to resolve and increasing the clarity and confidence we have in the conclusions that we reach."

Kyle Kennedy
Principal Security Engineer, Palo Alto Networks

Defining Your Use Cases

Well-defined use cases are the cornerstone of effective automation. Defining them involves identifying repetitive tasks, understanding business processes, and pinpointing pain points. Seek to:

- Engage stakeholders, analyze data, and prioritize use cases based on their impact and integration needs.
- Consider security and compliance requirements and select appropriate automation tools.

In essence, defining automation use cases is about identifying where automation can improve efficiency and effectiveness while aligning with organizational goals and compliance requirements. It's a structured process that ensures automation initiatives yield tangible benefits and contribute to operational excellence.

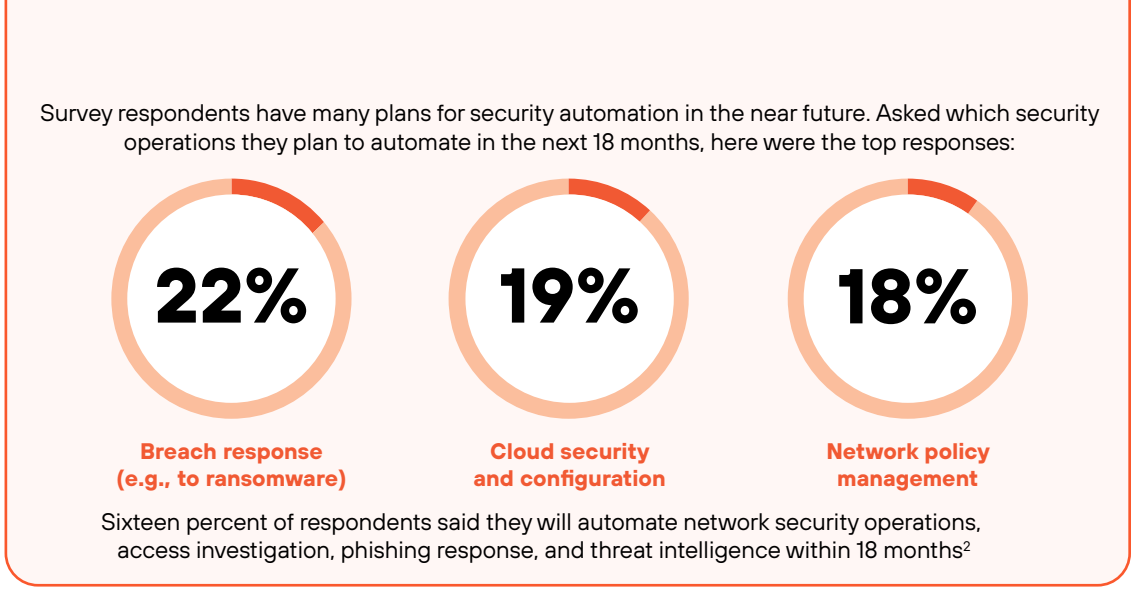


Figure 2: Incident response automation is happening

2. *The State of Security Automation*, Palo Alto Networks, December 2, 2021.

Clear Use Case Definition Avoids Scope Creep

It's crucial to define a clear use case scope. This step is vital in ensuring that your automation efforts remain focused, manageable, and effective. A precise use case definition is essential, starting with clear objectives and boundaries, such as addressing incident response for specific threats like phishing emails. This approach helps mitigate scope creep, a common pitfall in automation projects, preventing unnecessary complexity and feature additions.

Additionally, a well-defined scope aids in better risk assessment and management. It enables you to identify potential risks associated with the specific use case and plan mitigation strategies accordingly. This ensures that automation doesn't inadvertently introduce security vulnerabilities or compliance issues.

Example Use Cases: Phishing and Malware

Consider exploring example use cases like phishing and malware, which are among the most common security threats. Tailor these playbooks to your specific needs, and use them as templates for building your own.

Leveraging the Marketplace

The Cortex XSOAR marketplace is a treasure trove of prebuilt playbooks and automation resources. With over 1,000 packs available, chances are you'll find a prebuilt playbook equivalent to your needs. The marketplace content is based on extensive research, practical experience, customer feedback, and usage telemetry.

The development of marketplace content is an ongoing effort based on industry trends and feedback. By contributing your insights and experiences, you can help shape the future of security automation.

77%

of intrusions are suspected to be caused by three initial access vectors: **phishing**, **exploitation of known software vulnerabilities**, and **brute-force credential attacks**—focused primarily on remote desktop protocol (RDP).[3]

Selecting the Right SOAR Platform

Selecting the right SOAR platform is paramount in the journey toward efficient security automation; from having the ability to jump-start a playbook, yet also scale with you as you mature, adding more complexity, such as threat intelligence, into the platform. It also orchestrates across your entire security tool set, across functional teams and distributed networks, and is integrated with external threat intel for real-time visibility into threats impacting your environment.

3. *2022 Unit 42 Incident Response Report*, Palo Alto Networks, July 26, 2022.

How Cortex XSOAR Makes Life Easier for SecOps Teams

Accelerates Incident Response

By replacing low-level manual tasks with corresponding automations, security automation can shave off large chunks from incident response times while also improving accuracy and analyst satisfaction.

Standardizes and Scales Processes

Through stepwise, replicable workflows, security automation can help standardize incident enrichment and response processes that increase the baseline quality of response and is primed for scale.

Unifies Security Infrastructures

A SOAR platform like **Cortex XSOAR** can act as a connective fabric that runs through previously disparate security products, providing analysts with a central console from which to action incident response.

Increases Analyst Productivity

Since low-level tasks are automated, and processes are standardized, analysts can spend their time in more important decision-making and charting future security improvements rather than getting mired in grunt work.

Leverages Existing Investments

By automating repeatable actions and minimizing console switching, security orchestration enables teams to coordinate among multiple products easily and extract more value from existing security investments.

Streamlines Incident Handling

By applying automation to incident ticket management via integrations with key IT service management (ITSM) vendors such as ServiceNow, Jira, and Remedy, as well as communication tools such as Slack, security teams can speed up incident handling and closure. Incidents can also be distributed automatically to the respective stakeholders based on predefined incident types.

Improves Overall Security Posture

The sum of all aforementioned benefits is an overall improvement of the organization's security posture and a corresponding reduction in security and business risk.

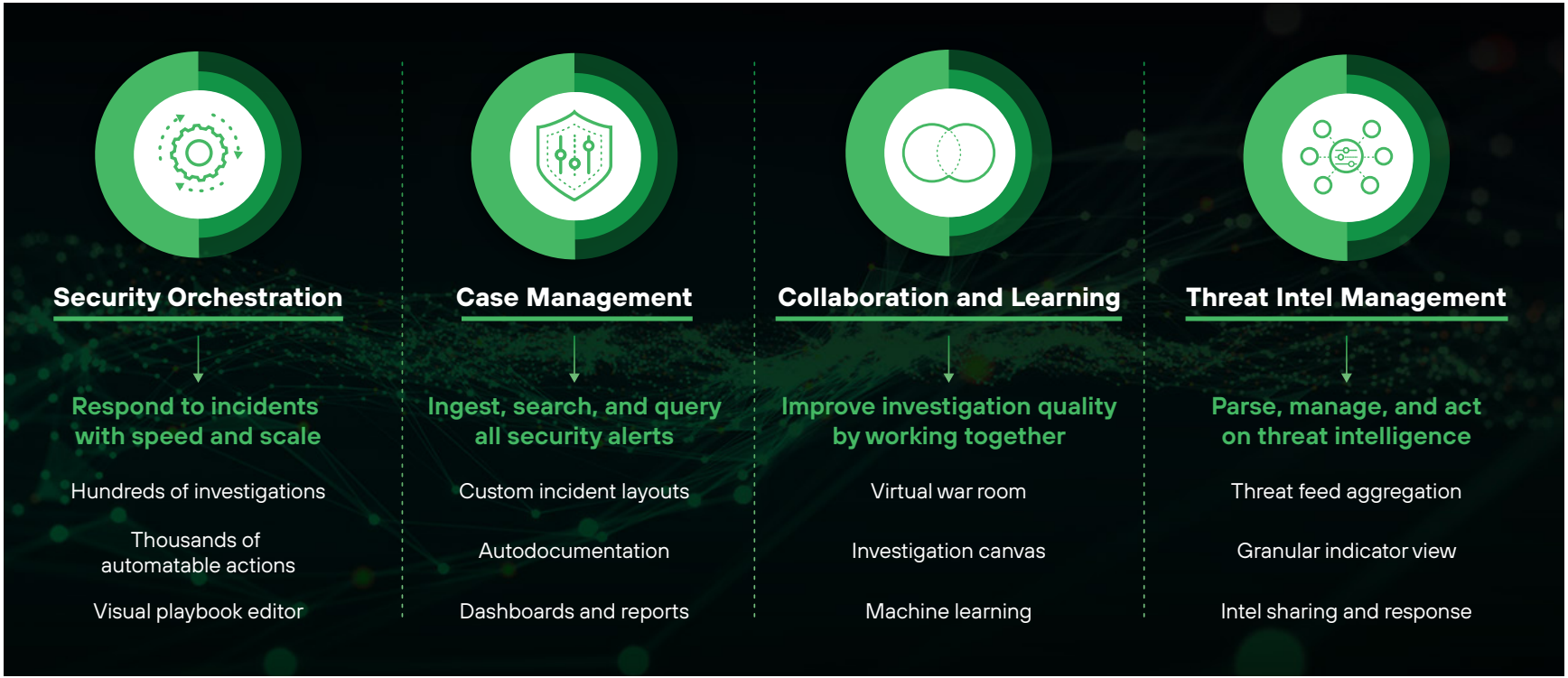


Figure 3: The pillars of a SOAR platform

Conclusion

The journey toward efficient security operations through automation is both exciting and rewarding. By investing in training, defining clear use case scopes, and leveraging out-of-the-box playbooks, you can take significant strides toward a more secure and efficient organization.

Additional Resources

For further reading and references, check out the recommended resources below:

Learn about Cortex XSOAR

Blog series: Playbook of the Week

Ready to demo Cortex XSOAR?

Infographic: State of Automation

Video: How Palo Alto Networks Uses Automation in Their SOC

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_eb_practical-guide-to-deploying-secops-automation_121223